BA

특1997-0064233

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.⁶
H04N 7/167

(43) 공개일자 1997년09월12일
(11) 공개번호 특1997-0064233

(21) 출원번호 특1996-0003723
(22) 출원일자 1996년02월15일

(71) 출원인 한국전자통신연구원 양승택
대전광역시 유성구 가정동 161번지 (우 : 305-350)

(72) 발명자 김신효
대전광역시 서구 삼천동 상록수아파트 103-708
윤성경
대전광역시 유성구 가정동 236-1
조진만
대전광역시 서구 월평동 진원아파트 101-805
이창원
대전광역시 유성구 전민동 나래아파트 108-602
조현숙
대전광역시 유성구 어은동 한빛아파트 131-1306
김동규
경기도 성남시 분당구 수내동 대림아파트 102-1301

(74) 대리인 박해천, 원석희

심사청구 : 있음

(54) 조건부 제한수신 서비스를 위한 메시지 처리 방법

요약

본 발명은 조건부 제한수신 서비스를 실현하기 위한 메시지 처리 방법에 관한 것으로서, 유료 방송에 필요한 제한수신 서비스를 위하여 송신 장치(1)에서 비화되어지기전에 자격 관리 메시지(EMM)와 자격 제어 메시지(ECM)를 암호화하여 전송하고, 수신 장치(2)에서는 허가된 사용자에게만이 분배된 정보를 복호화하는 과정을 통해 2 단계로 암호화하고, 이에 사용한 키값을 계속적으로 변경함으로써 키값의 안정성을 확보하여 해커나 불법 가입자로부터 비합법적인 시청을 막을 수 있는 효과가 있다.

대표도

도1

명세서

[발명의 명칭]

조건부 제한수신 서비스를 위한 메시지 처리 방법

[도면의 간단한 설명]

제1도는 본 발명이 적용되는 시스템 구성도,

제2도는 본 발명에 따른 매트릭스 방식에 의한 키 생성도

제3도는 본 발명에 따른 조건부 제한수신 서비스를 위한 메시지의 처리 흐름도.

본 내용은 요부공개 건이므로 전문 내용을 수록하지 않았음

(57) 청구의 범위

청구항 1

개개의 가입자의 자격을 부여하기 위해 자격 관리메시지인 EMM(Entitlement Management Message), 스크램블을 위해 필요한 제어 단어(CW), 제어단어(CW)를 암호화하여 자격 제어 메시지인 ECM(Entitlement

REF. 1 RCA 89131
CORRES. US/UK
COUNTRY Korea

Control Message)를 생성하여 추적하는 EMM/ECM 생성부(3), 상기 EMM/ECM 생성부(3)에서 입력된 제어 단어를 이용하여 방송 프로그램을 스크램블링하고, EMM/ECM 정보와 함께 다중화한 후, 전송 매체를 통해 수신된 데이터를 역다중화하여 출력하는 수신부(4)를 구비한 송신 장치(1)와; 전송 매체를 통해 수신된 데이터를 역다중화하여 출력하는 역다중화부(5), 자신이 수신할 데이터에 상기 역다중화부(5)에 제어 신호를 출력하여 역다중화한 후, EMM/ECM 정보를 추출하고, 제어 단어(CW)를 이용하여 수신한 스크램블링된 데이터를 디스크램블링하여 출력하는 프로세서(6), 상기 프로세서(6)에서 입력된 EMM에서는 분배를 복호화하고, 다시 이 분배키를 이용하여 세션키와 제어 단어(CW)를 EMM에서 추출하여 상기 프로세서(6)로 출력하는 스마트 카드(7)를 구비한 수신 장치(2)를 구비한 조건부 제한수신 시스템에서,

수신 장치(2)에서, 할당된 개인 키(PK), 그룹 키(GK), 적절 권한 키(DEK)를 생성하는 제1단계(100 내지 103); 상기 제1단계(100 내지 103)에서 생성된 개인 키(PK)와 그룹 키(GK)를 이용하여 마스터 개인키(MPK)를 암호화하여 키값 변경을 위한 EMM 메시지 생성 후, 수신측으로 송신하는 제2단계(104, 105); 상기 제1단계(100 내지 103)에서 생성된 적절 권한키(DEK)를 개인 키(PK)와 그룹 키(GK)를 이용하여 암호화하고, 권한 부여 EMM 메시지를 생성한 후, 수신측으로 송신하는 제3단계(106, 107); 및 제어 단어(CW)를 생성한 후, 적절 권한 키(DEK)를 이용하여 제어 단어(CW)를 암호화하여 자격 제어 메시지(ECM)를 생성하고, 제어단어(CW)를 이용하여 방송 프로그램을 스크램블링한 후 수신측에 송신하는 제4단계(108 내지 111); 을 포함하는 송신 과정과, 스마트 카드로부터 획득한 마스터 개인키(MPK)를 이용하여 수신한 키값 변경을 위한 EMM 메시지를 복호화하여 복호화된 데이터를 암호화 이전의 체크섬(CSUM)이 유효한지 판단하는 제5단계(200 내지 202); 상기 제5단계(200 내지 202)에서 유효하면 개인 키(PK), 그룹 키(GK)를 획득하고, 수신한 권한 여부EMM 메시지를 획득한 개인 키(PK), 그룹 키(GK)로 복호화하여 복호한 데이터의 CSUM이 유효한지 판단하는 제6단계(203 내지 205) ; 및 상기 제6단계(203 내지 205)에서 유효하면 적절 권한키(DEK)를 획득하고, 획득한 적절 권한 키(DEK)를 이용하여 수신한 ECM 메시지를 복호화하여 제어 단어(CW)를 획득하고, 상기 제어 단어(CW)를 이용하여 방송 프로그램을 디스크램블링하여 출력하는 제7단계(206 내지 208); 를 포함하는 수신 과정으로 이루어지는 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 2

제1항에 있어서, 상기 제1단계(100 내지 103)의 키 생성기에 입력되는 데이타는, 확장 키 인덱스 값으로부터 8바이트로 구성된 확장 키와 서비스 키인덱스 값으로부터 8바이트로 구성된 서비스 키를 이루어지는 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 3

제1항에 있어서, 권한 부여를 위한 EMM 메시지의 구조는, 메시지의 순서 번호를 나타내는 필드(Sequence), 다음 메시지의 존재 유무를 나타내는 필드(Append), 암호화시 홀수 또는 짝수 키를 사용 상태를 나타내는 필드(Encrypt)로 구성된 제어필드(CTRL)와, 벡터 갯수를 나타내는 필드(N)와, 벡터의 암호화에 사용된 키 번호를 나타내는 필드(KID)와, 채널 번호(ID), 홀수 서비스 키 주소(OSK), 짝수 서비스 키주소(ESK), 홀수 확장 키 주소(ODK), 짝수 확장 키 주소(EDK), 자격 만료 기간을 표시하고, 키 생성 메트릭스 번호를 나타내는 Expiry/KEM, 암호화 이전의 체크섬(checksum)을 나타내는 CSUM으로 구성된 다수의 암호화된 벡터 필드(Vector)로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 4

제1항에 있어서, 상기 키값 변경을 위한 EMM의 메시지의 구조는, 메시지의 순서 번호를 나타내는 필드(Sequence), 다음 메시지의 존재 유무를 나타내는 필드(Append), 암호화시 홀수 또는 짝수 키를 사용 상태를 나타내는 필드(Encrypt)로 구성된 제어 필드(CTRL)와, 벡터 갯수를 나타내는 필드(N)와, 벡터의 암호화에 사용된 키 번호를 나타내는 필드(KID)와, 변경될 키 번호를 나타내는 KID, 그룹 키일 경우 그룹 주소를 나타내는 BADDR, 홀수 서비스 키 주소(OSK), 짝수 서비스 키주소(ESK), 홀수 확장 키 주소(ODK), 짝수 확장 키 주소(EDK), 암호화 이전의 체크섬(checksum)을 나타내는 CSUM으로 구성된 다수의 암호화된 벡터 필드(Vector)로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 5

제1항에 있어서, 상기 자격 제어 메시지(ECM)의 구조는, 메시지의 순서 번호를 나타내는 필드(Sequence), 다음 메시지의 존재 유무를 나타내는 필드(Append), 암호화시 홀수 또는 짝수 키를 사용 상태를 나타내는 필드(Encrypt)로 구성된 제어 필드(CTRL)와, 벡터 갯수를 나타내는 필드(N)와, 다수의 벡터 필드(Vector)로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 6

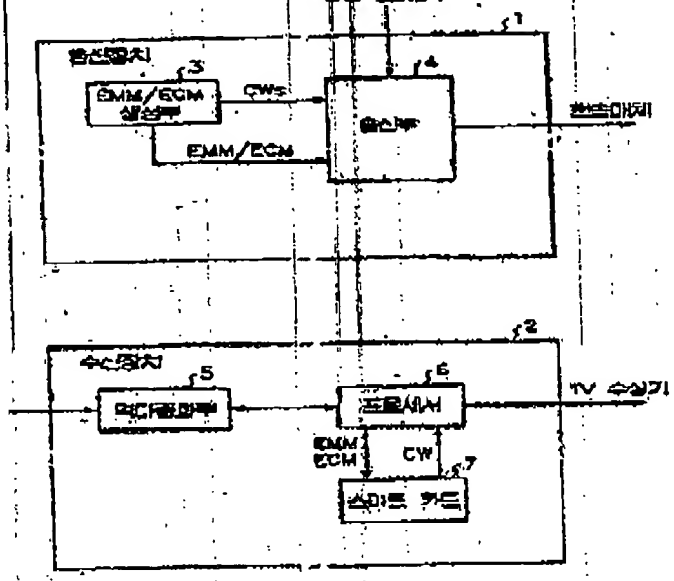
제5항에 있어서, 상기 벡터 필드(Vector)는, 채널번호(CH_ID), 채널 제어 필드(Chctrl), 홀수 제어 단어(ODW), 짝수 제어 단어(EDW), EPOCH 시간의 초단위 시간(time)과 채널의 형태(access), 현재 시스템 시간(month), 그리고, 암호화 이전의 체크섬(checksum) (csum)을 포함하는 필드로 구성된 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

청구항 7

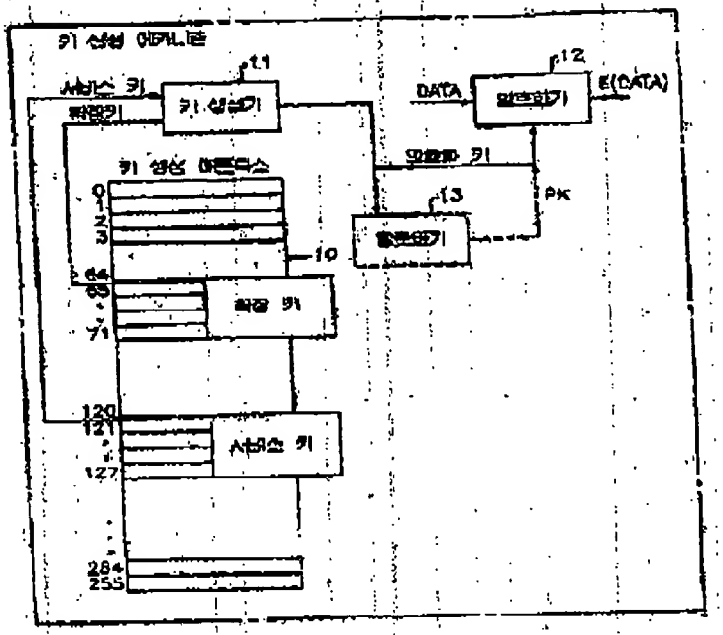
상기 ODW, EDW, time/access/month/csum은 암호화된 정보인 것을 특징으로 하는 조건부 제한수신 서비스를 위한 메시지 처리 방법.

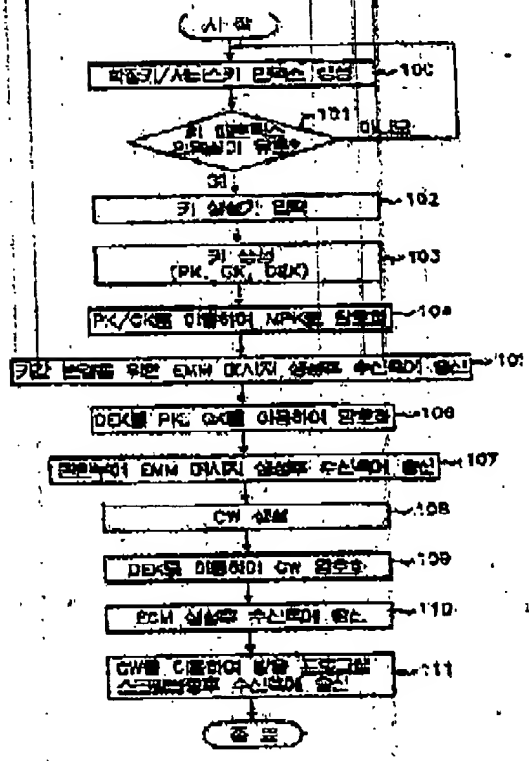
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면



도면2





도면6